STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Electronic Mail

Product ID: ENT-NET-042

Effective Date: November 2002

Approved: Scott Darkenwald, Director

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all state employees and state contractors using a state computer.

B. Purpose

The State provided electronic mail (email) system is to be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; and conducting other appropriate State business.

State employees are required to use the state provided email system for state business purposes unless they do not have a direct connection to SummitNet. Qualifying employee's use of an external email system must be approved by ITSD. Employees must use standard naming conventions for their email address when using an external email system.

All messages created, sent or retrieved, over the state's systems are the property of the State of Montana. Privacy of email is not guaranteed. Employees should not have expectations of privacy for any messages. Agency System Administrators, management, and Department of Administration personnel can monitor email for performance, troubleshooting purposes, or if abuses are suspected. Employees should use their best judgment in sending confidential messages over the email system. The use of encryption should be considered when sending these types of messages.

Employees will attend email training. For additional help with using email, the System Administrator should be contacted.

Stationery may be used when it enhances the business content of email. Stationery, moving graphics and/or audio objects should not be used unnecessarily since they consume more resources such as disk space, network bandwidth and tend to detract from the message content.

Unsolicited email, or Spam, should be forwarded to email address: virusreports@mt.gov for investigation before they are opened.

ITSD may block email from specified domains, from specific email addresses, or email that contains specific information in its subject line. These filters may be put into place because of their affect on the state's email system or computer

network. Email blocks will affect all users on the state's email system and must be approved by the State Chief Information Officer.

C. Misuse Of Email

The following items represent, but are not restricted to, misuse of state email resources:

- Circulating chain letters
- Using the state email system for: 1) "for-profit" activities, 2) "non-profit" or public, professional or service organization activities that aren't related to an employee's job duties, or 3) for extensive use for private, recreational, or personal activities.
- Statewide distributions of email. The system administrator should be contacted for correct procedures for large email distributions.
- Using personal email accounts, such as hotmail, outside of the state provided email system unless an exception has been granted.
- Other misuse activities as referenced in policy ENT-SEC-081 User Responsibilities.

D. Background - History On The Creation Of Or Changes To This Policy

This policy was originally created by the NetWare Managers Group Policy Committee. It was then modified to accommodate the migration to Microsoft Exchange. The policy was modified in October 2002 to address employee use of email systems other than Microsoft Exchange and to address Spam. These modifications were reviewed with the SummitNet Executive Council prior to adoption.

E. Guidelines - Recommendations, Not Requirements

Employees should check their mail with a frequency appropriate to their job duties and their departmental policy. If employees are unable to check their mail for an extended period of time, they should use the "auto reply" feature or make arrangements to have their mail picked up by someone else (supervisor, secretary, coworker) and reviewed to see if messages need a response.

If employees have a personal mailing list they feel would benefit the agency, they are encouraged to inform their System Administrator for the possibility of creating a public mailing list. Employees should use care and discretion when sending email to mailing lists and/or large groups. Sending a large file to multiple recipients could severely impact the network.

The chance of receiving a virus increases with the use of email. Many viruses come embedded in attachments. Suspicious email messages should be

forwarded to the State Information Security Manager for investigation before they are opened.

Employees should make judicious use of the features that increase email traffic and should strive to keep message and attachment sizes as small as possible. Use of graphics in auto-signatures or other parts of messages or attachments should be avoided because they greatly increase the size of a message. Use of the email text editor for simple messaging tasks is preferred since the same message created in a word processor is much larger. All attachments over one megabyte should be compressed (zipped) prior to sending.

All entities that use the state's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

Communications sent or received by the email system may be "documents" under Article II, Section 9 of the Montana Constitution or public records under Section 2-6-101, MCA, and should be generated and maintained accordingly. Employees should delete items from their in-tray and out-tray when they are no longer needed. If a mail item needs to be retained, it should be moved to an archive folder, a disk, or be printed. Items placed in an employee's archive are the employee's responsibility. The need for retention of an item should be reevaluated after it has been stored for 6 months. Employees can contact the State Records Manager with any questions on retention schedules.

In drafting and sending email messages, employees should not include anything they are not prepared for the public to read. Statements can potentially become a basis for litigation (e.g. sexual harassment comments) and/or civil or criminal liability. Email communication should resemble typical professional and respectful business correspondence.

F. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- §2-17-505(2), MCA
- §2-15-114, MCA
- 2-17-514(1) – Enforcement
- 2-17-512, MCA
- 2-17-534, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ENT-SEC-081 User Responsibilities.
- Internet Services Policy
- Computer Virus Detection and Prevention Policy
- Transmission Privacy Policy
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-NET-042
Proponent:	Scott Darkenwald, Director
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	November 2002
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.